AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method, comprising:

receiving a request for hardware component information at a service processor disposed in a hardware component as an open session request from a requesting client application;

transmitting from the service processor a challenge string to the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

receiving at the service processor a challenge response from the requesting client application, the challenge response including the session identification and a first hash number that ~~is~~ comprises a function of at least one of the challenge string, the session identification, a sequence number, and a password;

comparing the challenge response to an expected response to the challenge string, wherein the comparing includes verifying the session identification received in the challenge response against the session identification transmitted in the challenge string;

transmitting the hardware component information to the requesting client application; and

receiving at the service processor a direct platform control (DPC) message from the client application, the DPC message including a second hash number to verify the integrity of the DPC message, wherein the DPC message is to perform one or more of connecting to Basic Input Output System (BIOS), rebooting, resetting, and shutting down of the service processor.

Claims 2-3 (Canceled)

4. (Previously Presented) The method of claim 1, wherein the challenge response includes the sequence number, wherein the sequence number increments with every new message.

5. (Canceled)

6. (Currently Amended) The method of claim 1, further comprising examining the DPC message received from the client application for one or more of ~~the following:~~ the session identification, the sequence number, and the second hash number.

7. (Currently Amended) The method of claim 6, wherein the second hash number ~~is~~ comprises a function of at least one of a body of the DPC message, the session identification, the sequence number, and the password.

8. (Currently Amended) A method, comprising:

transmitting a request for hardware component information to a service processor disposed in a hardware component as an open session request from a requesting client application;

receiving from the service processor a challenge string at the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

transmitting to the service processor a challenge response from the requesting client application, the challenge response including the session identification and a first hash number that ~~is~~ comprises a function of at least one of the challenge string, the session identification, a sequence number, and a password;

receiving from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated in the service processor, wherein the comparison includes verifying the session identification in the challenge response transmitted to the service processor against the session identification received in the challenge string; and

receiving at the service processor a direct platform control (DPC) message from the client application, the DPC message including a second hash number to verify the integrity of the DPC message, wherein the DPC message is to perform one or more of connecting to Basic Input Output System (BIOS), rebooting, resetting, and shutting down of the service processor.

Claims 9-11 (Canceled)

12. (Currently Amended) The method of claim 8, wherein the second hash number ~~is~~ comprises a function of at least one of a body of the DPC message, the session identification, the sequence number, and the password.

13. (Currently Amended) An apparatus, comprising:

a remote access port; and

a service processor coupled to the remote access port, wherein the service processor including a machine-readable medium, having stored thereon a set of instructions which, when executed, cause the service processor to:

in response to a remote request for information about a component received as an open session request through the remote access port external to a host operating system of the apparatus, transmit a challenge string to a requesting client application, the challenge string including session identification assigned by the service processor, wherein the session identification is unique to each session;

compare a challenge response received from the requesting client application with an expected response, the challenge response including the session identification and a first hash number that ~~is~~ comprises a function of at least one of the challenge string, the session identification, a sequence number, and a password, wherein the comparing includes verifying the session identification received in the challenge response against the session identification transmitted in the challenge string;

transmit an authentication response to the requesting client application based on the comparison; and

receiving at the service processor a direct platform control (DPC) message from the client application, the DPC message including a second hash number to verify the integrity of the DPC message, wherein the DPC message is to perform one or more of connecting to Basic Input Output System (BIOS), rebooting, resetting, and shutting down of the service processor.

Claims 14-15 (Cancelled)

16. (Previously Presented) The apparatus of claim 13, wherein the service processor compares the sequence number included in the challenge response against previously received sequence numbers and ignores the challenge response if it does not include a sequence number in correct sequence.

17. (Previously Presented) The apparatus of claim 13, wherein the service processor compares the first hash number received in the challenge response with an expected hash calculated by the service processor and transmits a success or failure message depending upon a result of the comparison.

Claims 18-19 (Canceled)

20. (Currently Amended) A system, comprising:

a processor;

a memory; and

a client application stored on a machine-readable medium, the client application including a set of instructions which, when executed, cause the client application to:

transmit a request for hardware component information to a service processor disposed in a hardware component as an open session request;

receive from the service processor a challenge string at the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

transmit to the service processor a challenge response from the requesting client application, the challenge response including the session identification and a first hash number that ~~is~~ comprises a function of at least one of the challenge string, the session identification, a sequence number, and a password;

receive from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated at the service processor, wherein the comparison includes verifying the session identification received in the challenge response against the session identification in the challenge string; and

receiving at the service processor a direct platform control (DPC) message from the client application, the DPC message including a second hash number to verify the integrity of the DPC message, wherein the DPC message is to perform one or more of connecting to Basic Input Output System (BIOS), rebooting, resetting, and shutting down of the service processor.

21-30 (Canceled)

31. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, causes the machine to:

receive a request for hardware component information to a service processor disposed in a hardware component as an open session request;

transmit from the service processor a challenge string at the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

receive at the service processor a challenge response from the requesting client application, the challenge response including the session identification and a first hash number that ~~is~~ comprises a function of at least one of the challenge string, the session identification, a sequence number, and a password;

compare the challenge response to an expected response to the challenge string, wherein the comparing includes verifying the session identification received in the challenge response against the session identification transmitted in the challenge string;

transmit the hardware component information to the requesting client application; and

receiving at the service processor a direct platform control (DPC) message from the client application, the DPC message including a second hash number to verify the integrity of the DPC message, wherein the DPC message is to perform one or more of connecting to Basic Input Output System (BIOS), rebooting, resetting, and shutting down of the service processor.

Claims 32-33 (Canceled)

34. (Previously Presented) The system of claim 20, wherein the service processor compares the sequence number included in the challenge response against previously received sequence numbers and ignores the challenge response if it does not include a sequence number in correct sequence.

35. (Previously Presented) The system of claim 20, wherein the service processor compares a first hash number received in the challenge response with an expected hash calculated by the service processor and transmits a success or failure message depending upon a result of the comparison.

36. (Previously Presented) The machine-readable medium of claim 31, wherein the sequence number included in the challenge response increments with every new message.

37. (Currently Amended) The machine-readable medium of claim 31, wherein the set of instructions which, when executed by the machine, further causes the machine to examine each packet received from the client application for one or more of ~~the following:~~ the session identification, the sequence number, and the first hash number.

38. (Previously Presented) The method of claim 12, wherein the sequence number increments with every new message.